Table of Contents

Security & Logging In

Security Overview

All NAS users play an important role in safeguarding their own data and NASA resources. The following articles are organized to assist you in a) getting familiar with security-related terminology and NAS security policies and guidelines; and b) performing the necessary steps in order to successfully and safely log into NAS systems.

Security Terminology, Policies, and Guidelines

- Secure Shell (SSH)
- Role of the Secure Front-Ends
- Two-Factor Authentication and Policy
- RSA SecurID Fobs
- Password Creation Rules
- Public/Private Key Pairs
- Acceptable Use Statement
- Account Policies

Steps for Logging In to NAS Systems

- Enabling SecurID Fob and First Time Login to a Secure Front-End
- Subsequent Logins to HECC Systems
- Two-Step Connection Using SecurID+Password for the SFEs
- Setting Up Public Key Authentication
- Two-Step Connection Using SecurID+Publickey for the SFEs
- Setting Up SSH Passthrough
- One-Step Connection Using Publickey and Passthrough
- Pleiades Front-End Load Balancer
- Common Login Failures or Issues
- Post Login Issues

Data Handling Information

Once you are connected to a NAS system, follow the policies and guidelines in the articles below when handling your data.

- ITAR/Export Control
- Files and Directories Permissions Policies
- SUID/SGID Scripts

Secure Shell

The SSH protocol is used for both interactive login sessions and executing arbitrary commands on remote systems. It provides secure, encrypted communication between two untrusted hosts over an insecure network. Users must prove their identities to successfully connect to a remote system. Both the authentication information, such as a password or passcode, as well as data are encrypted over the network.

SSH uses a client-server model. On the client, users initiate an SSH connection with the *ssh* command, which connects to the *sshd* daemon on the remote system.

OpenSSH

All NAS systems, except the secure front-ends, use the OpenSSH implementation of the SSH protocol.

This implementation includes *ssh, scp, sftp, sshd,* and utilities such as *ssh-add, ssh-agent,* and *ssh-keygen*. On the secure front-ends, a commercial implementation of the SSH server is used, but OpenSSH is used for the SSH client.

Although OpenSSH includes support for both SSH protocol 1 and protocol 2, all NAS systems accept only connections using protocol 2.

Please be aware that there are both security and performance issues with older versions of OpenSSH. NAS users are strongly recommended to use **OpenSSH 5.2 or later** for best performance, security, and functionality.
Both Mac OS X and most Linux distributions include a version of OpenSSH. However, it is important to keep up with the latest security updates for your operating system to ensure that you have the latest version of OpenSSH supported by the vendor.

On systems running the Windows operating system, please ensure that a client supporting SSH protocol 2 is installed. We recommend using Cygwin (a Linux-like environment for Windows) and OpenSSH. Follow the instructions in the PDF file Installing cygwin/openssh for more details.

To learn more about OpenSSH, see the **ssh(1)** and **ssh_config(5)** man pages.

The following Wikipedia pages have additional information on SSH:

- http://en.wikipedia.org/wiki/Secure_Shell
- http://en.wikipedia.org/wiki/OpenSSH
- http://en.wikipedia.org/wiki/Cygwin

Role of the Secure Front-Ends

The secure front-end (SFE) systems for the secure enclave are designated SFE1 and SFE2. The enclave includes all high-end systems such as Pleiades, Columbia, hyperwall-2, and Lou.

To access IT resources inside the enclave, you must first use SSH to connect to either one of the SFEs and authenticate using two factors (SecurID+password or SecurID+publickey). Once authenticated, you can then use SSH on the SFEs to access any of the NAS systems.

Note that SSH from the SFEs to hosts outside of the enclave is not allowed.

Two-Factor Authentication and Policy

DRAFT

This article is being reviewed for completeness and technical accuracy.

What is two-factor authentication?

In the field of security, there are three general ways you can prove you are who you claim to be. Each way is called a "factor." The factors fall into the categories of (1) something you have, such as an ATM card, (2) something you know, such as the personal pin to your bank account, and (3) something you are, such as your fingerprint. Two-factor authentication refers to using any two of these factors to authenticate a person before access to systems is granted.

NAS Policy

At NAS, the three different factors used are:

1. your assigned RSA SecurID fob (sometimes called a key fob or a token)
2. your password to the NAS systems
3. your public/private key pair

You are required to authenticate yourself with two of these factors before you can access NAS resources from outside the NAS HECC Enclave. One of these two factors has to be the possession of your SecurID fob. Thus, you can authenticate yourself with a combination of either SecurID + password, or SecurID + public/private key pair.

Two-factor authentication is required when accessing

- the secure front-end systems, SFE1 and SFE2, from your local desktop systems
- any system inside the NAS HECC Enclave (such as Pleiades or Columbia) from your localhost using SSH Pasthrough.
- Bouncer or Bruiser (bastion hosts to other NAS desktop systems) from your local desktop systems
- Return to Flight (RTF) hosts through the web

Related articles: RSA SecurID Fob, Passwords, Public/Private Key Pairs

RSA SecurID Fobs

An RSA SecurID fob is mailed to each new NAS user, and is required to log into the NAS systems. The fob is a way of identifying yourself by proving you have something (fob) and you know something (your PIN). For continuing users, a new fob is mailed when the old one expires.

In December 2004, NASA's Office of the Chief Information Officer (CIO) directed the agency to secure its supercomputing facilities with the RSA Security Inc.'s SecurID technology.

Fob Description

RSA's SecurID fob is an electronic device that generates a time-based pseudo-random number (called the tokencode) every 30 seconds, and presents the tokencode via its LCD display. When used in conjunction with a personal identifying number (PIN), the pair is used to authenticate account access, such as login. This is known as One Time Password (OTP) technology.

The front face of a NAS-provided fob presents an LCD displaying six digits. The digits displayed will change every 30 seconds. Left of the six digits, six bars are displayed. These bars act as the countdown timer for the current token code displayed. Each of the six bars disappear at regular intervals until all bars are gone, at which point a new random number will be displayed and six bars re-appear to restart the countdown process.

The back side of a fob has three identifiers:

- Serial Number: This numerical sequence is unique for each fob
- Expiration Date: The "mm/dd/yy" format identifies the battery's termination date
- Mfr's Lot Number: The manufacturer's batch identifier

Fob Care

Do not expose the fob to extreme temperature, pressure, x-rays, or magnetic fields.

If you fob is damaged or lost, immediately contact the NAS Control Room at 800-331-8737 or 650-604-4444. A Control Room analyst will initiate steps to replace your fob. Expect typical postal delivery delays. In addition, the analyst will issue you a set of 10 passwords (each usable only once and in combination with your PIN). You may request another set if the initial set is used before you receive your new fob.

More information about RSA SecurID can be found at http://www.rsa.com/

Related Articles

Enabling Your SecurID Fob and First-Time Login

Password Creation Rules

DRAFT

This article is being reviewed for completeness and technical accuracy.

Your password is vulnerable to attack since it can be guessed. Follow the rules below when creating your NAS passwords:

1. Never use a password at NAS that has ever been used by you anywhere else, and never use the password that you create for NAS anywhere else, ever.

2. A password must contain a minimum of 8 characters. It must contain one character each from at least three of the following character sets: uppercase letters, lowercase letters, numbers, and special characters.

3. Use non-trivial passwords; examples of "trivial" passwords that you may not use include but are not limited to:

    - your user ID
    - a dictionary word of any language or a dictionary word with numbers appended or prepended to it
    - a password either wholly or predominately composed of the following: user ID, owner name, birthdate, Social Security Number, family member or pet's name, name spelled backwards, or other personal information
    - a contractor name
    - a division or branch name
    - repetitive or keyboard patterns (for example, "abc#ABC", "1234", "qwer", "mnbvc", "aaa#aaaa")
    - the name of any automobile or sport team
    - the name of any vendor product or nickname for a product
4. A new password can not be any one of your last 24 passwords.

5. Once you are successful in changing a password, you have to wait at least 7 days to change it again.
6. Passwords must be changed every 90 days.

Never share your password with anyone. For more information, read Account Policies and the Acceptable Use Statement.

Password Information and Policies

DRAFT

This article is being reviewed for completeness and technical accuracy.

This article outlines the processes and rules for getting your default password and changing your password.

Obtaining Your Password

If you are a new user and don't know your default installation password for the NAS high-performance computing systems, please call the NAS Control Room at 1-800-331-USER (8737) or 1-650-604-4444.

If you already have an account on a NAS system, and you are approved to get an account on another machine, your password on the new machine is your current "lou" password. If you do not remember this password, a Control Room analyst will provide you with a new default password.

NOTE: Due to security requirements, you must provide the Control Room analysts with a) the correct answer to a security question that you have already submitted to NAS, or b) the analyst must be able reach you at the phone number listed on your account request form. If your phone number has changed due to office moves or reorganizations, your PI must contact the Control Room stating the reason for the change via phone or FAX. The FAX number is 650-604-1777. If your PI is unavailable, your branch chief or division chief may do this for you.
Once you have been given a default password, you will be prompted to change it once you log in to a NAS system.

Password Creation Rules

Your password is vulnerable to attack since it can be guessed. Follow the rules below when creating your NAS passwords:

1. Never use a password at NAS that has ever been used by you anywhere else, and never use the password that you create for NAS anywhere else, ever.

2. A password must contain a minimum of 12 characters. It must contain one character each from at least three of the following character sets: uppercase letters, lowercase letters, numbers, and special characters.

3. Use non-trivial passwords; examples of "trivial" passwords that you may not use include, but are not limited to:

    - your user ID
    - a dictionary word of any language or a dictionary word with numbers appended or prepended to it
    - a password either wholly or predominately composed of the following: user ID, owner name, birthdate, Social Security Number, family member or pet's name, name spelled backwards, or other personal information
    - a contractor name
    - a division or branch name
    - repetitive or keyboard patterns (for example, "abc#ABC", "1234", "qwer", "mnbvc", "aaa#aaaa")
    - the name of any automobile or sport team
    - the name of any vendor product or nickname for a product
4. A new password cannot be any of your last 24 passwords.

5. Once you are successful in changing a password, you have to wait at least 7 days to change it again.
6. Passwords must be changed every 60 days.

Never share your password with anyone. For more information, see Account Policies and the Acceptable Use Statement.

Public/Private Key Pairs

DRAFT

This article is being reviewed for completeness and technical accuracy.

Public-key authentication is a means of identifying yourself by proving that you know the private key associated with a given public key. This method is more secure than password authentication, but it requires more effort to set up.

Public-Key Basics

To use this method, you use the *ssh-keygen* program to generate a public/private key pair on your local system. You will be prompted for a passphrase which is used to encrypt the private key. By default, the private key is stored in *~/.ssh/id_rsa* and the public key is stored in *~/.ssh/id_rsa.pub*.

The private key should only be kept on your local system and should be encrypted using a passphrase that is at least as strong as any password you would normally use. The security of this method depends on keeping the private key safe and secure.

The public key can be safely copied to other systems and appended to *~/.ssh/authorized_keys* on those systems. The server uses this copy of the public key to confirm that you possess the private key.

When you authenticate to a server using public-key authentication, the SSH client offers a copy of the public key to the server and the server then compares it against the keys listed in your *~/.ssh/authorized_keys* file. If it matches, the server indicates that it is able to proceed with the authentication. At that point, the SSH client will prompt you for the passphrase in order to decrypt the private key. The private key is then used to sign a message that includes data specific to the SSH session. The server can then use its copy of the public key to verify the signature.

If the server can verify the signature, you are authenticated.

Why are public/private keys more secure than passwords?

- The passphrase is never sent over the network.
- The private key is never sent over the network.
- It is extremely computationally expensive to derive the private key from the public key.
- Protects against man-in-the-middle attacks.

Related Articles

Setting Up Public Key Authentication

Acceptable Use Statement

This document gives the requirements for use of the computing systems, resources and facilities located at and/or operated by the NASA Advanced Supercomputing (NAS) Division at NASA Ames Research Center.

As a user of the computing systems, resources and facilities located at and/or operated by the NASA Advanced Supercomputing (NAS) Division at NASA Ames Research Center, I agree to the following and understand that failure to abide by these provisions may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution:

1. NAS accounts are to be used only for the purpose for which they are authorized and are not to be used for non-NASA related activities.
2. Unauthorized use of the computer accounts and computer resources to which I am granted access is a violation of Federal law; constitutes theft; and is punishable by law (Section 799, Title 18, U.S. Code). I understand that I am the only individual to access these accounts and will not knowingly permit access by others without written approval. I understand that sharing passwords with other people, even on the same project, is prohibited. I understand that my misuse of assigned accounts and my accessing others' accounts without authorization is not allowed. I understand that this/these system(s) and resources are subject to monitoring and recording and I will have no expectation of privacy in my use of these systems
3. I am responsible for using the computing systems, resources and facilities in an efficient and effective manner. I understand that account deactivation will result after 60 days of non-use and data will be deleted after 90 days unless my project or I make arrangements with the NAS User Services to preserve my data.
4. I understand that these computing systems are unclassified systems. Therefore, processing and storing classified, or other information that requires safeguarding in the interest of National Security, is prohibited.
5. I understand that these computing systems are categorized as moderate according to FIPS 199, therefore processing and storing information that is categorized as high according to FIPS 199 and NIST SP 800-60 is prohibited.
6. I understand that I am responsible for protecting any information processed or stored in my accounts and will take appropriate precautions to protect Sensitive But Unclassified information (e.g., proprietary information or information subject to International Traffic in Arms Regulations or Export Control Regulations), which may include encrypting the data to provide protection that goes beyond the standard OS protection provided by the computing systems.
7. I understand that I shall not engage in activities that compromise or weaken the security of the NAS systems or have been identified as prohibited and high-risk practices by the NAS Security Team. These activities include but are not limited to keeping unauthorized world-writable directories, running password cracking programs, downloading or introducing malicious software, running unauthorized P2P and VOIP software and copying or making available system and password configuration files to others.

8. I understand that I shall not make copies of copyrighted software, except as permitted by law or by the owner of the copyright.
9. I understand that I shall not attempt to access any data or programs contained on systems for which I do not have authorization or explicit consent from the owner of the data/program, the NAS Division Chief or the NAS Computer Security Official.
10. I understand that I am required to report any security weaknesses in the systems or any IT security incidents including misuse or violation of this agreement, to the NAS User Services, support@nas.nasa.gov, or to the NAS Security Team, security@nas.nasa.gov.
11. I understand that I am required to access the NAS Computers only from remote systems which are fire walled and are running regularly updated virus protection software.
12. I understand that I will be required to complete the NASA mandatory Basic IT Security Training available at: http://satern.nasa.gov/. (Note: Additional details are available from NAS User Services.)
13. If applicable, I further agree to abide by the provisions NASA NPD 2540.1F regulating privileges and responsibilities of NASA employees and contractors.

Account Policies

DRAFT

This article is being reviewed for completeness and technical accuracy.

Users are responsible for being aware of the general account-related policies below.

- Both users and NAS staff requesting either a new or a renewed account must complete the Basic IT security training **annually** and fill out an Account Request form for the annual NOP (new operational period).
- Users shall not share their account(s) with anyone. This includes sharing the password to the account, providing access via an .rhost entry or other means of sharing.
- Users are responsible for protecting any information used and/or stored on/in their accounts.

Account Deactivation

Users who do not comply with the rules listed in the Acceptable Use Statement will have their accounts disabled either temporarily or permanently. Account deactivation will result after 90 days of non-use (by changing user's normal shell to noshell) and data may be archived after 120 days of non-use.

Enabling Your SecurID Fob and First-Time Login

Follow the steps below to enable your SecurID fob, obtain a password, select your personal identification number (PIN), and then use your fob to log into the NAS secure front-end systems for the first time.

Step 1: Enable Fob and Password

Your SecurID fob has been sent in a *disabled* state. To enable your fob, call the NAS Control Room (650-604-4444 or 1-800-331-8737).

A Control Room analyst will confirm your identity by asking you a security question that you submitted with your account request form, or by calling you back at your work phone number on record.

The analyst will then enable your fob, setting it in New PIN Mode. If you are a first-time user, an initial default password will also be provided to you when you call to enable your fob.

Step 2: Complete the New-PIN Process

`IMPORTANT: Before you begin Step 2, your computer must be set up to log in using SSH.`

The first time you log in to any of the secure front-end machines (SFE1 and SFE2, or the bastion hosts, Bouncer and Bruiser) you will set up a Personal Identification Number (PIN) and complete a two-factor authentication process. You will be prompted to choose a PIN or to have a PIN automatically selected for you. To complete the new-PIN process:

- Log in using SSH:

  ```
  your_localhost% ssh machine.nas.nasa.gov
  ```

  where machine is *sfe1, sfe2, bouncer* or *bruiser*

  If your usernames on your localhost and NAS systems are different, then type the following:

  ```
  your_localhost% ssh nas_username@machine.nas.nasa.gov
  ```

  If you get a message that indicates an "ssh_known_hosts" error, the simple solution below works for many users. Once fixed, you should not have to do this again in subsequent SSH sessions. Sfe1 is used in the example below:

  ```
  your_localhost% ssh -o "stricthostkeychecking=ask" sfe1.nas.nasa.gov

  ----------------------------------------------------------------
  ```

```
The authenticity of host 'sfe1.nas.nasa.gov (198.9.4.3)'
can't be established.  RSA key fingerprint is
11:9f:ae:09:56:2d:45:66:8e:9a:df:15:52:d6:88:5e.
Are you sure you want to continue connecting (yes/no)? yes

----------------------------------------------------------------
Warning: Permanently added 'sfe1.nas.nasa.gov,198.9.4.3' (RSA) to
the list of known hosts.
```

- At the prompt "Enter PASSCODE," enter the six-digit tokencode displayed on the fob.

```
----------------------------------------------------------------
PAM authentication
Enter PASSCODE:
```

- At the next prompt, select whether to create your own PIN (4 to 8 numbers or letters with *no* special characters) or to have one created for you (type "yes" or "no"). In either case, memorize your PIN. Never write down your PIN.

```
----------------------------------------------------------------
PAM authentication
You may create your own PIN or accept a server assigned PIN.
Would you like to create your own new PIN (yes/no)?
PAM authentication
Enter your new PIN (4 to 8 digits or characters)
New PIN:
Confirm new PIN:

Never divulge your PIN. No NAS staff member will ever ask you
for your PIN. If you think someone may have learned your PIN,
call the NAS Control Room at 650-604-4444 or 800-331-8737.
```

- Wait for the tokencode displayed on your fob to change, then enter your PIN, followed immediately by the tokencode, and hit RETURN.

  For example, if your PIN is "d70l398" and your fob displays the tokencode "052993" then enter "d701398052993" and hit RETURN. Note that you can use either a lowercase or an uppercase "D" because PINs are not case sensitive.

```
----------------------------------------------------------------
PAM authentication
Wait for token to change, and enter PASSCODE:
```

  The new-PIN process is now complete, although you may not get clear confirmation on your screen. Currently, PINS do not expire, but this could change in the future.

  Continue to Step 3 to log in to sfe1, sfe2, bouncer or bruiser using the two-factor authentication process.

Step 3: Complete First-time Two-factor Authentication

Now that you have completed the new-PIN process, the system will prompt you to log in using two-factor authentication for the first time.

- At the prompt asking for your PASSCODE, enter your PIN followed immediately by the tokencode displayed on the fob.

- At the prompt, enter your NAS password.
- If you are a first-time user, after entering your password you will need to change your password. For more information on choosing a password read the Password Creation Rules.

You are now authenticated, and can log into other systems at the NAS facility on which you have an account.

NOTE: Each tokencode displayed on your fob can be used just once. If you have to authenticate twice (for example, because you mistyped your password), you must wait for your fob to display a new tokencode, and then re-enter the new PASSCODE.

Subsequent Logins to HEC Systems

Once you successfully enable your RSA SecurID fob and log in for the first time to one of the secure front-ends (SFEs), such as sfe1 *or* sfe2, you can follow one of the approaches below for all subsequent logins to the systems in the secure enclave:

- Two-Step Connection Using SecurID+Password for the SFEs

  This is the quickest and easiest way to access the SFEs and then connect to any of our systems without doing any extra setup.
- Two-Step Connection Using SecurID+Publickey for the SFEs

  This method requires that you first set up public key authentication. Once that is done, you can use SecurID + Public key to access the SFEs and then connect to any of our systems in two steps.
- One-Step Connection Using Publickey and Passthrough

  This method requires that you first set up public key authentication and set up SSH passthrough. Once this is done correctly, you can access any of the systems in what appears to be a single step.

Two-Step Connection Using SecurID+Password for the SFEs

DRAFT

This article is being reviewed for completeness and technical accuracy.

If you have your NAS password and the SecurID fob enabled, you can use SecurID + password for the two-factor authentication to the SFEs. In this case, connection from your localhost to a system inside the NAS HECC Enclave (such as Pleiades, Columbia or Lou) is done in two steps: first usig SSH from your localhost to one of the SFEs, and then using SSH again from the SFE to the system inside the enclave.

Step 1: Accessing the SFEs

For accessing SFE1 or SFE2 from your localhost, type the command:

```
your_localhost% ssh username@sfe1.nas.nasa.gov
```

or

```
your_localhost% ssh username@sfe2.nas.nasa.gov
```

Username is your NAS login name. If you have the same username for your localhost and the NAS systems, you can omit "username@" in the above commands.

By typing one of the above commands, you will be connected to either SFE1 or SFE2 and prompted for your SecurID passcode followed by a password prompt. Your password for the SFEs is the same as your Lou password.

Step 2: Accessing HECC systems

For accessing a system inside the enclave, for example, Lou1, from either SFE1 or SFE2, type the command:

```
sfe1 or sfe2% ssh lou1
```

You will be prompted for your Lou password.

Setting Up Public Key Authentication

DRAFT

This article is being reviewed for completeness and technical accuracy.

Follow the steps below to set up for public key authentication.

1. **Creating SSH Public/Private Key Pair**

   To use public key authentication with the SFEs, you need to have a SSH public/private key pair. If you do not, you can create a SSH public/private key pair by typing the following command and following the prompts:

   ```
   your_localhost% ssh-keygen -t rsa
   Generating public/private rsa key pair.
   Enter file in which to save the key (/Users/username/.ssh/id_rsa):RETURN
   Enter passphrase (empty for no passphrase):enter a passphrase of your choice
   Enter same passphrase again: type your passphrase again
   Your identification has been saved in /Users/username/.ssh/id_rsa.
   Your public key has been saved in /Users/username/.ssh/id_rsa.pub.
   ```

   Your passphrase for the private key must meet NASA password requirements.

   If you are using a non-Unix system, please consult your SSH documentation.

2. **Converting OpenSSH Key to Commercial SSH Key (optional)**

   If you used OpenSSH or your SSH client created an OpenSSH public/private key pair, you may wish to convert the public key to work with the commercial SSH that is installed on the SFEs. To convert your public key, type the following command (your exact filenames may differ, *id_rsa.pub* and *id_rsa_sfe.pub* are example filenames):

   ```
   your_localhost%ssh-keygen -e -f ~/.ssh/id_rsa.pub >
   .ssh/id_rsa_sfe.pub
   ```

   ```
   This step was recommended when an older version of commercial
   SSH server was used on SFEs, which did not support the key
   format used by OpenSSH. The current version of commercial SSH
   server on SFEs does support OpenSSH key format. Thus, this
   step is optional.
   ```

3. **Copying SSH Public Key to SFEs**

   Copy the public key file to your *~/.ssh2* directory on the SFEs (for example, SFE1).

If you have done step 2 above, use the command

```
your_localhost%scp ~/.ssh/id_rsa_sfe.pub
username@sfe1.nas.nasa.gov:.ssh2
```

On the SFEs, type the following command

```
sfe1%echo "Key id_rsa_sfe.pub" > .ssh2/authorization
```

If you skip step 2 above, use the command

```
your_localhost%scp ~/.ssh/id_rsa.pub
username@sfe1.nas.nasa.gov:.ssh2
```

On the SFEs, type the following command

```
sfe1%echo "Key id_rsa.pub" > .ssh2/authorization
```

Please note, only use one space between the word Key and the public key filename.

To test your public/private key pair, type the following command on your localhost:

```
your_localhost%ssh -i ~/.ssh/id_rsa username@sfe1.nas.nasa.gov
```

You will be prompted for both your SecurID passcode and your private key passphrase.

```
Setting up public key authentication for both SFE1 and SFE2 gives
you the freedom of using either one.
```

Two-Step Connection Using SecurID+Publickey for the SFEs

DRAFT

This article is being reviewed for completeness and technical accuracy.

If you have set up public key authentication for one or both of the SFEs, connection from your localhost to a system inside the NAS HECC Enclave (such as Pleiades, Columbia or Lou) is done in the following two steps. SFE1 is used in the example.

Step 1: Accessing the SFEs

For accessing SFE1 from your localhost, type the command:

```
your_localhost% ssh username@sfe1.nas.nasa.gov
```

Username is your NAS login name. If you have the same username for your localhost and the NAS systems, you can omit "username@" in the above commands.

By typing the above command, you will be connected to SFE1 and prompted for your SecurID passcode and your private key passphrase.

Step 2: Accessing HECC systems

For accessing a system inside the enclave, for example, Lou1, from SFE1, type the command:

```
sfe1% ssh lou1
```

You will be prompted for your Lou password.

Setting Up SSH Passthrough

The passthrough feature on the secure front-ends allows you to log into a system in the enclave by typing just one SSH command. The most useful way to use passthrough is with public key authentication and an SSH agent.

Once you set this feature up correctly, then each time you use SSH from your localhost to log into a NAS high-end computing system, you will be prompted for only the SecurID passcode. The SSH agent forwarding and an SSH passthrough program handle the public key authentication for you, so you will not be prompted for the passphrase of your private/public keys.

To configure passthrough using public key authentication, follow the 3 steps described in Setting Up Public Key Authentication for the SFEs. You must also copy your public key to any system in the enclave to which you want to connect using passthrough, and you need to edit the *.ssh/config* file on your localhost. Detailed information on these steps are linked below:

1. **Create SSH Public/Private Key Pair**
2. **Convert OpenSSH Key to Commercial SSH Key** (optional)
3. **Copy SSH Public Key to SFEs**
4. **Copy OpenSSH Public Key to Hosts Inside the Enclave**

   Hosts inside the enclave use OpenSSH, so you will need to copy the OpenSSH version of your public key to the hosts inside the enclave and place the key in your *.ssh/authorized_keys* file.

   Note: The permission for the *authorized_keys* file must be set to 600. Group/others write permissions on */u/username* and */u/username/.ssh* are not allowed for public key authentication.

   The following example uses lou.nas.nasa.gov as the enclave host. If you want SSH passthrough to work for other hosts inside the enclave, then repeat the steps below for each one.

   - **Copy your OpenSSH public key**

     On your localhost, type:

     ```
     your_localhost% scp ~/.ssh/id_rsa.pub
     username@sfe1.nas.nasa.gov:
     ```

     Note: *.ssh* is a directory. If it does not exist, make sure that you create a *.ssh* directory first before issuing the command below. Otherwise, it will copy the file *id_rsa.pub* to lou1 with the filename *.ssh*.

On SFE1, type:

```
sfe1% scp id_rsa.pub username@lou1:.ssh
```

- **Add your OpenSSH public key to your *.ssh/authorized_keys* file**

On your localhost, type:

```
your_localhost% ssh username@sfe1.nas.nasa.gov
```

On SFE1, type:

```
sfe1% ssh username@lou1
```

The *username* is your NAS login name.

On lou.nas.nasa.gov, type:

```
lou1% cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
```

```
Note: If you get the error
      /u/username/.ssh/authorized_keys: No such file or directory
after issuing the command above, likely, you have "set noclobber"
which prevents you from overwriting files. You can do "unset noclobber"
first to avoid this problem.
```

5. **Modify .ssh/config File on Your Local Host**

In your *~/.ssh/config* file on your localhost, add the entries for the hosts inside the enclave you want to access. If you do not have the *~/.ssh/config* file, create a new file called *config* in your *~/.ssh* directory and add the entries.

Template for .ssh/config

For your convenience, you can download a NAS template (a text file) for the *.ssh/config* file (attached at the end of this page). The contents of this file are also shown below. Sfe1 is used in this template. You can switch to using sfe2 if you wish to use sfe2 for SSH passthrough. Also remember to replace <NAS_login_name> with your NAS username before use.

This template should work for users who use this file only for accessing NAS systems. It this applies to you, use this template and continue with the instructions in **Step 6**.

```
Host sfe
# Replace sfe1 by sfe2 if sfe1 is unavailable
HostName                sfe1.nas.nasa.gov
```

```
Host sfe sfe?.nas.nasa.gov
Ciphers                 aes128-cbc,aes192-cbc,aes256-cbc,3des-cbc
ForwardAgent            no
MACs                    hmac-sha1

Host sfe sfe?.nas.nasa.gov dmzfs?.nas.nasa.gov sup*.nas.nasa.gov
LogLevel                info
ProxyCommand            none

Host pfe pfe-last pfe.nas.nasa.gov pfe-last.nas.nasa.gov
HostKeyAlias            pfe1.nas.nasa.gov
ProxyCommand            ssh -oCompression=no sfe /usr/local/bin/ssh-balance %h

# Add additional hosts to the list below as needed
Host *.nas.nasa.gov lou lou? cfe? pfe? bridge? sfe pfe pfe-last
ForwardAgent            yes
HostbasedAuthentication no
Protocol                2
ProxyCommand            ssh -oCompression=no sfe /usr/local/bin/ssh-proxy %h
ServerAliveInterval     10m

# Replace  with your NAS username
User                    <NAS_login_name>

# Enabling compression may improve performance for slow connections
#Compression            yes

# Uncomment this line if you are using OpenSSH 4.7 or later
#MACs                   umac-64@openssh.com,hmac-md5,hmac-sha1
```

Instructions for Creating Your Own .ssh/config

If you use your *.ssh/config* file for accessing both NAS systems and systems at other sites, you can add entries on top of the template discussed earlier. The entries take the form:

```
Host hostname
ProxyCommand ssh username@hostname.nas.nasa.gov /usr/local/bin/ssh-proxy hostname
```

Hostname is the name of the host you want to access. It can be the abbreviated hostname (such as *pfe1*) or the fully-qualified domain name (such as *pfe1.nas.nasa.gov*). Note that using bbftp requires the fully qualified domain name, thus it is a good idea to include both.

6. **Set Up SSH Agent**

Ssh-agent is a program to hold and manage the private key on your localhost and respond to key challenges from remote hosts. The private key is initially not stored in the agent and is added through the *ssh-add* program.

Ssh-agent is typically started in the beginning of an X session or a login session and you provide your passphrase to unlock your private key for this originiating session. For any outbound SSH connection to a remote host (for example, SFE1 or SFE2) made from this original session, the SSH agent remembers your private key and will respond to challenges automatically without prompting you to type in your passphrase again.

If you want to use SSH to connect from the first remote host (e.g., SFE1, SFE2) to a second remote host (e.g., pfe1) and possibly from the second remote host to a third remote host, a feature called **agent forwarding** allows a chain of SSH connections to forward all the key challenges back to the original agent, thus eliminating the need of using password or public/private keys for these connections.

In order for agent forwarding to work, your public key has to be installed already in all the remote hosts that you intend to connect to.

Instructions for UNIX or LINUX systems

- If you use csh or tcsh, to launch *ssh-agent*, type the following command

  ```
  your_localhost% eval `ssh-agent -c`
  ```

  If you use sh or bash, to launch *ssh-agent*, type the following command

  Example:

  ```
  your_localhost% eval `ssh-agent -s`
  ```

- To add your private key to ssh-agent, type the following command

  ```
  your_localhost% ssh-add private_key
  ```

  Example:

  ```
  your_localhost% ssh-add ~/.ssh/id_rsa
  Enter passphrase for /Users/username/.ssh/id_rsa: type your passphrase
  ```

One-Step Connection Using Publickey and Passthrough

DRAFT

This article is being reviewed for completeness and technical accuracy.

This method requires Setting Up Public Key Authentication and Setting Up SSH Passthrough first. Once done correctly, use the command below to connect from your localhost to a system inside the HECC Enclave with one single use of SSH:

```
your_localhost% ssh username@hostname
```

Hostname is one of the hosts you listed in your *~/.ssh/config* file, for example, pfe[1-12], bridge[1-2], cfe2, lou[1-2], etc.

Username is your NAS username. If you have the same username for your localhost and the NAS systems, you can omit "username@" in the above commands.

Example:

```
your_localhost% ssh pfe1
PAM Authentication
Enter PASSCODE: type in your passcode
pfe1%
```

Pleiades Front-End Load Balancer

DRAFT

This article is being reviewed for completeness and technical accuracy.

There are 12 front-end nodes to the Pleiades super-cluster, namely, pfe1 - pfe12. To provide a load balanced front-end environment for all users of Pleiades, a mechanism has been created to automatically pick the least loaded system from among pfe1 - pfe12 for a user login. The system load is a weighted function of disk, processor, and network loads. The load balancer is invoked using the special hostname pfe (or pfe.nas.nasa.gov) instead of the explict pfe1 - pfe12 when logging in via SSH.

In some instances, there may be a need to log into the last Pleiades front-end accessed from a given host. For example, the user may have started a long-running process on a particular front-end such as a VNC session. In this case, the special hostname pfe-last (or pfe-last.nas.nasa.gov) may be used. This hostname will connect the user to the last front-end they accessed from the same host (e.g. from sfe1).

The usage of this mechanism is described below. These examples assume that you want to login via sfe1. Change it to sfe2 if you want to use sfe2 instead.

- If you normally login to a Pleiades front-end (pfe[1-12]) in two steps (first login to sfe[1,2], then login to pfe[1-12]), you can simply do the following to connect to the least loaded Pleiades front-end:

  ```
  your_localhost% ssh sfe1 (or ssh sfe1.nas.nasa.gov)
  sfe1% ssh pfe (or ssh pfe.nas.nasa.gov)
  ```

  or, if you use different usernames on your localhost and on NAS systems,

  ```
  your_localhost% ssh username@sfe1 (or ssh username@sfe1.nas.nasa.gov)
  sfe1% ssh username@pfe (or ssh username@pfe.nas.nasa.gov)
  ```

  If you want to connect to the last front-end you connected to via sfe1, do:

  ```
  your_localhost% ssh sfe1 (or ssh sfe1.nas.nasa.gov)
  sfe1% ssh pfe-last (or ssh pfe-last.nas.nasa.gov)
  ```

  or, if you use different usernames on your localhost and on NAS systems,

  ```
  your_localhost% ssh username@sfe1 (or ssh username@sfe1.nas.nasa.gov)
  sfe1% ssh username@pfe-last (or ssh username@pfe-last.nas.nasa.gov)
  ```

  Note that you will be prompted for a password on the pfeN (N=1 to 12) system chosen for you by the load balancer.

- If you normally login to a Pleiades front-end using SSH Passthrough, add the following in the *~/.ssh/config* file of your localhost.

```
Host pfe pfe-last pfe.nas.nasa.gov pfe-last.nas.nasa.gov
ProxyCommand ssh sfe1.nas.nasa.gov /usr/local/bin/ssh-balance %h
HostKeyAlias pfe1.nas.nas.gov
HostbasedAuthentication no
```

or, if you use different usernames on your localhost and on NAS systems,

```
Host pfe pfe-last pfe.nas.nasa.gov pfe-last.nas.nasa.gov
ProxyCommand ssh username@sfe1.nas.nasa.gov /usr/local/bin/ssh-balance %h
HostKeyAlias pfe1.nas.nas.gov
HostbasedAuthentication no
```

Note the use of *ssh-balance* instead of the traditional *ssh-proxy* used for passthrough.

The first time your use this method, you will need to add the usual -o "StrictHostKeyChecking=ask" to populate the host key. That is,

```
your_localhost% ssh -o "StrictHostKeyChecking=ask" pfe (or
pfe.nas.nasa.gov)
```

After the key has been populated, to connect to the least loaded Pleiades front-end, simply do:

```
your_localhost% ssh pfe (or ssh pfe.nas.nasa.gov)
```

To connect to the last front-end you connected to from a particular sfe, do:

```
your_localhost% ssh pfe-last (or ssh pfe-last.nas.nasa.gov)
```

Pleiades and bbFTP

Due to the manner in which bbftp operates, it is not possible to perform bbftp transfers to the Pleiades load balancer (i.e. pfe or pfe-last). Instead, you must select a specific front-end for the transfer (e.g. pfe4). Scp, sftp, and rsync transfers will work normally with the load balancer.

Common Login Failures or Issues

DRAFT

This article is being reviewed for completeness and technical accuracy.

- **SSH Known-Hosts Error**

  SSH offers the ability to verify the identity of the remote host to which you are connecting. A successful host verification indicates that your SSH client has estabilished a secure connection with the SSH server and no intermediate machines have access to that connection.

  The identity of the remote host can be verified by checking the host public key of the remote host stored either in the system-wide */etc/ssh/ssh_known_hosts* file (or */etc/ssh_known_hosts* for some systems) or your personal *~/.ssh/known_hosts* file on your localhost.

  SSH has three ways it can react to an unrecognized or changed SSH host key, based on the value of the *StrictHostKeyChecking* variable in either the system-wide */etc/ssh/ssh_config* file (or */etc/ssh_config* for some systems) or your personal *~/.ssh/config* file :

  - `StrictHostKeyChecking=no`

    This is the most insecure setting as it will blindly connect to the server. It will add the server's key if it's not present locally, and if the key has changed it will add the key without asking.
  - `StrictHostKeyChecking=ask`

    With this setting, if you have no host key for the server, it will show you the fingerprint and ask you to confirm. If you connect and the key does not match, it will prevent you from logging in, and will tell you where to find the conflicting key inside the *known_hosts* file.
  - `StrictHostKeyChecking=yes`

    This is the most secure setting. If you have no host key for this server, then it will prevent you from logging in at all.

  If *StrictHostKeyChecking* is set to *yes* and you get errors similar to the following the first time you log in to one of the SFEs, the simple solution is to add **-o "stricthostkeychecking=ask"** in your ssh command. Sfe1 is used in this example.

  Sample Error:

```
your_localhost% ssh sfe1.nas.nasa.gov

WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
11:9f:ae:09:56:2d:45:66:8e:9a:df:15:52:d6:88:5e.
Please contact your system administrator.
Add correct host key in /Users/userid/.ssh/known_hosts2 to get rid
of this message.
Offending key in /etc/ssh_known_hosts2:24
RSA host key for sfe1.nas.nasa.gov has changed and you have
requested strict checking.
No RSA host key is known for sfe1.nas.nasa.gov and you have
requested strict checking.
Host key verification failed.
```

Solution:

```
your_localhost% ssh -o "stricthostkeychecking=ask" sfe1.nas.nasa.gov

-----------------------------------------------------------------
The authenticity of host 'sfe1.nas.nasa.gov (198.9.4.3)'
can't be established.
RSA key fingerprint is
11:9f:ae:09:56:2d:45:66:8e:9a:df:15:52:d6:88:5e.
Are you sure you want to continue connecting (yes/no)? yes
-----------------------------------------------------------------
Warning: Permanently added 'sfe1.nas.nasa.gov,198.9.4.3' (RSA) to
the list of known hosts.

-----------------------------------------------------------------
Plugin authentication
Enter PASSCODE: type your passcode
```

- **Common SecurID Passcode Problems**
  - ♦ If you cannot log in after you created your new PIN,

```
your_localhost% ssh sfe1
user@sfe1's password:
Authenticated with partial success.
Plugin authentication
Enter PASSCODE:
Plugin authentication
You may create your own PIN or accept a server assigned PIN.
Would you like to create your own new PIN (yes/no)? yes
Plugin authentication
Enter your new PIN (exactly 8 alphanumeric characters)
New PIN:
Confirm new PIN:
Plugin authentication
Enter PASSCODE:
```

```
Plugin authentication
Enter PASSCODE:
Permission denied, please try again.
user@sfe1's password:
Permission denied, please try again.
user@sfe1's password:
Permission denied ().
```

it is possibly that you did not successfully complete the "New-Pin Process". You might have used a special character in your PIN. Your PIN MUST consist of **EXACTLY 8 alphanumeric characters**, with at least one letter and at least one number, but no special characters.

- Each SecurID 6-digit tokencode can be used only once. If you try to use a tokencode that has just been used, you will be prompted again to enter a new passcode.

```
your_localhost% ssh sfe1.nas.nasa.gov
PAM Authentication
Enter PASSCODE: enter PIN and a tokencode which was just used
PAM Authentication
Enter PASSCODE: ener PIN and a new token code
```

- If you failed to provide a correct PIN + tokencode in a few consecutive attempts, your SecurID fob will be temporarily disabled. NAS Help Desk can help you unlock your fob (even for fobs provided by your local center). Call NAS Help Desk at 1-800-331-USER (8737) or 1-650-604-4444 for assistance.

- **Common Passthrough Problems**

If you set up SSH passthrough correctly, you should be prompted for your SecurID passcode only, and be transferred to the desired host. The following describes a few common problems and their solutions:

- If the authentication failed when you entered the passcode, it is possible that you have different usernames between your localhost and the NAS systems and you did not include your NAS username in your *.ssh/config* file.

  There are two ways to include your NAS username in the *.ssh/config* file:

  - If you use the *.ssh/config* file for connecting to multiple computer sites, then you should add your NAS username to the ProxyCommand lines for corresponding NAS hosts. For example:

    ```
    Host lou1
    ProxyCommand ssh username@sfe1.nas.nasa.gov /usr/local/bin/ssh-proxy
    ```

    In this case, you will still need to issue your ssh command as the following example in order to avoid being prompted for a password:

    ```
    %ssh nas_username@lou1
    ```

◊ If you use the *.ssh/config* file only for connecting to NAS, then you can simply add the following at the beginning of your *.ssh/config* file:

`User nas_username`

You do no need to add your NAS username to the ProxyCommand line. In addition, you can simply use the following command and won't be prompted for a password:

```
%ssh lou1
```

♦ If you are prompted for password in addition to the passcode, there are multiple possible causes:

◊ As described above, you may have a different username and need to use

```
your_localhost% %ssh nas_username@lou1
```

◊ Either your home directory or the *.ssh/authorized_keys* file under your NAS account have write permission for group or others. You need to correct the permission so that they have write permission only to you.

◊ Either one or both of the following files is missing:

· *.ssh2/authorization* of sfe[1,2]
· *.ssh/authorized_keys* of the NAS HECC host that you want to connect to

♦ If you are prompted for passphrase in addition to the passcode, likely, you did not use the commands "ssh-agent" and "ssh-add ~/.ssh/id_rsa" to forward your private key before you issue the ssh command.

• **Incorrect Ciphers**

A cipher is an algorithm for performing encryption or decryption. The SSH client and server must have a matching cipher in order to successfuly verify the keys. If you get an error similar to the following:

```
no matching cipher found: client blowfish-cbc
server aes128-cbc,aes192-cbc,aes256-cbc,3des-cbc
```

check your *./ssh/config* file or */etc/ssh/ssh_config* file on your localhost and add the appropriate ciphers.

```
To modify /etc/ssh_config, system administrator's privilege
may be needed.
```

- **Password Expiration**

  Your NAS password is valid for 90 days. An email is sent to you by NAS reminding you to change your password. If it has expired, you can still log in. However, you will be prompted to change it right away.

  ```
  This policy will change from 90 days to 60 days in the near
  future.
  ```

- **Account Expiration or Deactivation**

  Your NAS account is active if you have a valid project and a valid account request form on file at NAS. If your account has expired, it will be removed from NAS database and the */etc/passwd* files. When this happens, no login will be allowed.

  Please note that the account request form has to be filled out once every year. When the form has expired, you should receive an email from the NAS account administrator asking you to fill out a new one.

  If you violate NAS security rules such as those listed in the Acceptable Use Statement, your account can be deactived.

Post Login Issues

DRAFT

This article is being reviewed for completeness and technical accuracy.

- **Idle SSH connections are broken after 10-15 minutes**

  If you find that idle SSH connections tend to be dropped after 10 to 15 minutes and your are using a router or other device that implements Network Address Translation (NAT), such as a DSL router, you may want to enable the *ServerAliveInterval* parameter in your *~/.ssh/config*.

  The issue is that some devices that implement NAT will drop information from their state tables if a TCP connection has been idle for just a few minutes. In such cases, it may be necessary to ensure that the connection is never truly idle for an extended period.

  The *ServerAliveInterval* parameter (supported in OpenSSH 3.8 and later) causes the SSH client to periodically send an encrypted query to determine if the server is still responsive. The packets will make the connection appear to be active and can prevent the NAT state table entry for the connection from timing out.

  For example, adding the following to your *~/.ssh/config* will cause an encrypted query to be sent every five minutes:

  ```
  ServerAliveInterval 5m
  ```

  ```
  NOTE: You may need to experiment with the length of the
  interval to determine an appropriate value to prevent your
  connection from being broken. If you use the NAS config
  template, ServerAliveInterval is set to 10 minutes.
  ```

- **SSH connection is periodically broken even when connection is active**

  During an SSH session, the client and server will re-negotiate the keys used to encrypt the session every so often. Very old versions of OpenSSH did not implement this feature, which can cause a problem when connected to the SFEs. Your connection may appear to hang or may abort with an error message such as the following:

  ```
  Dispatch protocol type 20
  ```

  If you encounter this issue, you will need to upgrade to a newer version of OpenSSH.

NOTE: Other implementations that were derived from the OpenSSH distribution, such as SUN Secure Shell, are likewise known to exhibit this problem.

- **Slow performance transferring data**

  While OpenSSH performs reasonably for local data transfers, the performance will tend to be reduced due to the latency of long-haul network connections.

  Depending on the severity of the impact you may have several options to improve this situation.

  1. Upgrade to OpenSSH 4.7 or later

     If you are using a version of OpenSSH that is older than 4.7, you may see an improvement in file transfer performance by upgrading to OpenSSH 4.7 or later. This is due to the use of a larger channel buffer introduced in that version.

  2. Use an HPN-enabled version of OpenSSH

     The High-Performance Networking (HPN) patch set maintained by the Pittsburgh Supercomputing Center (PSC) allows the channel buffer used by OpenSSH to grow as needed. This may be useful in cases where OpenSSH 4.7 does not yield satisfactory performance.
  3. Enabling compression

     In cases where you are seeing very poor performance (under 1.2 MB/s) and the data you are transferring will compress well, you may wish to enable compression.

     You can do this by adding -C to your scp or sftp command-line.

  Read Tips for File Transfers for more recommendations.

ITAR/Export Control

DRAFT

This article is being reviewed for completeness and technical accuracy.

The PI must, by law, manage, protect and control the export of the project's data in a way that complies with the security category of the data. There are five categories of data:

- Mission Information (MSN)
- Business and Restricted Technology Information (BRT)
- Scientific, Engineering, and Research Information (SER)
- Administrative Information (ADM)
- Public Access Information (PUB)

```
Mission Information requires the most stringent security control
and protection. Currently, the NAS Facility is not configured to
provide services for MSN data. For Business and Restricted
Technology Information (which includes ITAR/Export Control Data),
no world access (write/read/execute) is allowed.
```

Detailed descriptions of each data categories are as follows:

Mission Information (MSN)

If the information, software applications, or computer systems in this category are altered, destroyed, or unavailable, the impact on NASA could be catastrophic. The result could be the loss of major or unique assets, a threat to human life, or prevention of NASA from preparing or training for a critical Agency mission. Examples in this category are those that control or directly support one of the following:

1. Human space flight
2. Wide Area Networks
3. Development of the data or software used to control human flight
4. Training simulation vehicles
5. Wind tunnel operations
6. Launch operations
7. Space vehicle operations

Business and Restricted Technology Information (BRT)

This category consists of information that NASA is required by law to protect. It includes information, software applications, or computer systems that support the Agency's business and technological needs. In general, if information in this category should be disclosed inappropriately, the disclosure could result in damage to our employees, in loss of business

for our partners and customer businesses, in contract protest, or the illegal export of technology. This category includes systems containing technological information that is restricted from general public disclosure because of public laws. Examples in this category are those that are related to the following kinds of information:

1. Financial
2. Legal
3. Payroll
4. Personnel
5. Procurement
6. Source selection
7. Proprietary information entrusted to the Government
8. Export controlled technical information (includes disclosure to foreign nationals)

Scientific, Engineering, and Research Information (SER)

All official NASA information held by NASA employees may be released publicly only in accordance with NASA regulations; however, systems in this category do not contain information for which the release is otherwise governed by law. This category consists of information that supports basic research, engineering, and technology development but is less restricted against public disclosure.

1. Alteration, destruction, unauthorized disclosure, or unavailability of the systems, application, or information would have an adverse or severe impact on individual projects, scientists, or engineers; however, recovery would not impede the Agency in accomplishing a primary mission.
2. Integrity is the driving concern in this category followed by availability. Confidentiality is important and should be considered in a risk assessment insofar as it protects individual researchers from such things as premature disclosure of their work by another party. The impact, however, is primarily on an individual rather than on the Agency.

Administrative Information (ADM)

Administrative Information includes, but is not limited to electronic correspondence, briefing information, project/program status, infrastructure design details, predecisional notes, vulnerability descriptions, passwords, and internet protocol addresses. Organizations run various applications-from problem reports to configuration management tools-on administrative IT systems.

1. This category includes systems, applications, and information that support NASA's daily activities, such as electronic mail, forms processing, networking, and management reporting.
2. Integrity and availability are the driving IT security concerns. The impact is primarily managerial in nature, which would require time and resources to correct. Confidentiality may be of concern in certain specific administrative information. In

such instances, additional security controls must be imposed as a risk analysis dictates.

Public Access Information (PUB)

This category includes information, software applications, and computer systems specifically intended for public use or disclosure, such as a public web site or hands-on demonstrations. The loss, alteration, or unavailability of information in this category would have little direct impact on NASA's missions but might expose the Agency to embarrassment, loss of credibility, or public ridicule.

1. Information posted for public access which could expose NASA missions to risk if compromised should be afforded additional protective measures. In these cases, the baseline requirements for ADM information should be implemented. (For example, contractors may submit proposals based on information from NASA web sites. Loss, alteration, or unavailability of data at the site could result in protests, thereby impacting procurement cycle time and ultimately NASA missions.)
2. Integrity and availability are the driving concerns. IT security controls are selected to protect the resources themselves and are not intended to protect the confidentiality of the information.

Files and Directories Permissions Policies

DRAFT

This article is being reviewed for completeness and technical accuracy.

Write permission is granted only to the file owner. That is, files and directories may not be writable by group and/or others unless there is a valid justification. By default, files and directories are set with owner permissions.

To request write permissions for members of your group or others, your principal investigator (PI) must submit a valid justification by calling 1-800-331-USER or 1-650-604-4444, or by sending an e-mail to support@nas.nasa.gov. The request will be reviewed by the NAS security officer.

For directories, if a world write permission is approved by the security officer, the "sticky bit" must be set also (chmod +t) on that directory to prevent an unprivileged user from deleting or renaming files of other users in that directory.

File and directory permissions are routinely scanned for violation of this policy. For those files/directories that are permitted by the security officer to be writable by group and/or others, they will be recorded on an exception list.

SUID/SGID Scripts

DRAFT

This article is being reviewed for completeness and technical accuracy.

Users are prohibited from creating and using privileged SUID and/or SGID scripts under their home, scratch, nobackup and /tmp filesystems.

SUID scripts (that is, with permission u+s) and SGID scripts (with permission g+s) could allow someone (other than the owner) to gain unauthorized access to users' files, posing a security hazard.

The high end computing systems at the NAS facility are configured to disable the execution of any SUID/SGID shell scripts.